AguasdelCesar
S.A. E.S.P.

POLÍTICA DE SEGURIDAD DIGITAL 2026 - 2029

TABLA DE CONTENIDO

Contenido

1. INTRODUCCIÓN

La Política de Seguridad Digital de AGUAS DEL CESAR S.A. E.S.P. establece el marco de referencia integral para la protección de los activos de información, la infraestructura tecnológica y los servicios digitales que soportan la gestión misional de la entidad en la prestación de los servicios públicos de Agua Potable y Saneamiento Básico en el Departamento del Cesar.

En el contexto actual, donde la transformación digital y el uso intensivo de las tecnologías de la información y las comunicaciones (TIC) son fundamentales para la operación eficiente de los servicios públicos domiciliarios, resulta imperativo contar con un instrumento que defina las directrices, principios, roles y responsabilidades en materia de seguridad de la información, ciberseguridad y privacidad de los datos.

Esta política se enmarca dentro del Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad y se alinea con el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones, la Política Nacional de Seguridad Digital (CONPES 3854 de 2016), la norma técnica ISO/IEC 27001:2013, la ISO 31000:2018 y demás normatividad vigente aplicable.

AGUAS DEL CESAR S.A. E.S.P., consciente de su responsabilidad como entidad prestadora de servicios públicos esenciales y de la necesidad de salvaguardar la información de sus usuarios, funcionarios y partes interesadas, se compromete a gestionar de manera sistemática los riesgos de seguridad digital, promoviendo una cultura organizacional orientada a la protección de la confidencialidad, integridad y disponibilidad de su información.

2. OBJETIVO GENERAL

Definir las políticas, principios, directrices y lineamientos de seguridad digital que deben seguir todos los servidores públicos, contratistas, proveedores y terceros de AGUAS DEL CESAR S.A. E.S.P., con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información, en el marco del Sistema de Gestión de Seguridad de la Información (SGSI) y la Política Nacional de Seguridad Digital.

2.1 Objetivos Específicos

- Establecer un marco de referencia para la gestión de la seguridad de la información alineado con la norma ISO/IEC 27001:2013 y el MSPI.
- Proteger los activos de información de la entidad contra amenazas internas y externas, deliberadas o accidentales.
- Crear una cultura de ciberseguridad y concientización en todos los niveles de la organización.
- Reducir el impacto de los riesgos de seguridad digital mediante la implementación de controles adecuados.
- Garantizar el cumplimiento de la normatividad legal vigente en materia de seguridad de la información, protección de datos personales y transparencia.
- Gestionar de manera sistemática y cíclica los riesgos de seguridad digital en las actividades de la entidad.

3. ALCANCE

La presente Política de Seguridad Digital es aplicable a todos los niveles y procesos de AGUAS DEL CESAR S.A. E.S.P., incluyendo los procesos estratégicos, misionales, de apoyo y de evaluación y control. Su cumplimiento es obligatorio para:

- Todos los servidores públicos de la entidad, independientemente de su tipo de vinculación.
- Contratistas y consultores que presten sus servicios a la entidad.
- Proveedores y terceros que tengan acceso a la información o a los sistemas de información de la entidad.
- Operadores de servicios tecnológicos y de telecomunicaciones.

Esta política aplica a toda la información creada, procesada, almacenada, transmitida o utilizada por la entidad, sin importar el medio, formato, presentación o lugar en el cual se encuentre, abarcando información física, digital, verbal y visual.

El alcance incluye los sistemas de información que soportan la operación de los servicios de acueducto, alcantarillado y aseo, los sistemas administrativos y financieros, las plataformas de atención al usuario, la infraestructura de red y comunicaciones, así como los sistemas de control y monitoreo operacional, donde aplique.

4. COMPROMISO DE LA ALTA DIRECCIÓN

La Gerencia General de AGUAS DEL CESAR S.A. E.S.P. se compromete a:

- Liderar y apoyar la implementación, mantenimiento, seguimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).
- Garantizar la asignación de los recursos financieros, tecnológicos y humanos necesarios para la gestión de la seguridad digital.
- Incluir la seguridad de la información en las decisiones estratégicas de la entidad.
- Promover el cumplimiento de los requisitos legales aplicables en materia de seguridad de la información y protección de datos personales.
- Fomentar la cultura de seguridad de la información y la capacitación constante de los colaboradores.
- Asegurar la revisión periódica de la política, cuando se presenten cambios significativos en el contexto interno o externo.

5. PRINCIPIOS RECTORES

La gestión de la seguridad digital en AGUAS DEL CESAR S.A. E.S.P. se fundamenta en los siguientes principios:

- **Confidencialidad:** Se garantiza que la información sea accesible únicamente por personas, entidades o procesos debidamente autorizados.
- **Integridad:** Se salvaguarda la exactitud, completitud y veracidad de la información y sus métodos de procesamiento, evitando modificaciones o alteraciones no autorizadas.
- **Disponibilidad:** Se asegura que los usuarios autorizados tengan acceso oportuno a la información y a los recursos tecnológicos relacionados cuando lo requieran.
- **Privacidad:** Se protegen los datos personales de los titulares de la información conforme a la Ley 1581 de 2012 y sus decretos reglamentarios.
- **Legalidad:** Todas las actuaciones en materia de seguridad digital se enmarcan en el ordenamiento jurídico colombiano vigente.
- **Proporcionalidad:** Las medidas de seguridad implementadas son proporcionales a los riesgos identificados y al valor de los activos de información protegidos.
- **Responsabilidad compartida:** La seguridad digital es responsabilidad de todos los servidores, contratistas y partes interesadas de la entidad.
- **Mejora continua:** El SGSI se revisa, evalúa y mejora de manera permanente para adaptarse a los cambios en el entorno de amenazas y a las necesidades de la organización.
- **Gestión basada en riesgos:** Las decisiones de seguridad se adoptan con base en la identificación, análisis, evaluación y tratamiento sistemático de los riesgos de seguridad digital.

6. MARCO NORMATIVO

La presente política se sustenta en el siguiente marco normativo y de referencia:

Ítem	Norma / Referencia	Descripción
1	Constitución Política de Colombia	Artículos 15 y 20. Derecho a la intimidad, protección de datos personales y libertad de expresión.
2	CONPES 3854 de 2016	Política Nacional de Seguridad Digital.
3	Ley 1273 de 2009	Delitos informáticos. Protección de la información y de los datos.
4	Ley 1341 de 2009	Principios y conceptos sobre la sociedad de la información y organización de las TIC.
5	Ley 1581 de 2012	Disposiciones generales para la protección de datos personales.
6	Ley 1712 de 2014	Transparencia y acceso a la información pública.
7	Ley 1928 de 2018	Aprobación del Convenio sobre la Ciberdelincuencia (Convenio de Budapest).
8	Ley 1955 de 2019	Plan Nacional de Desarrollo. Componente de transformación digital.
9	Decreto 1078 de 2015	Decreto Único Reglamentario del Sector TIC.
10	Decreto 1008 de 2018	Lineamientos generales de la política de Gobierno Digital.
11	Decreto 1377 de 2013	Reglamentación parcial de la Ley 1581 de 2012 (Datos Personales).
12	Decreto 620 de 2020	Lineamientos para servicios ciudadanos digitales.
13	Decreto 338 de 2022	Actualización de la Política de Gobierno Digital.
14	Resolución 500 de 2021 MinTIC	Lineamientos y estándares para la estrategia de seguridad digital y adopción del MSPI.
15	Resolución 1519 de 2020	Estándares sobre transparencia, accesibilidad web y seguridad digital.
16	NTC/ISO/IEC 27001:2013	Requisitos para Sistemas de Gestión de Seguridad de la Información.
17	NTC/ISO/IEC 27002:2013	Código de prácticas para controles de seguridad de la información.

18	NTC/ISO/IEC 27005	Directrices para la gestión de riesgos de seguridad de la información.
19	NTC/ISO 31000:2018	Gestión del Riesgo. Principios y directrices.
20	Guía DAFP V5	Guía para la administración del riesgo y diseño de controles en entidades públicas.
21	MSPI	Modelo de Seguridad y Privacidad de la Información de Gobierno Digital.

7. DEFINICIONES

- **Activo de información:** Cualquier elemento que tenga valor para la organización, incluyendo información, software, hardware, servicios, personas e intangibles relacionados con el tratamiento de datos.
- **Amenaza:** Causa potencial de un incidente no deseado que puede causar daño a un sistema o a la organización.
- **Ciberseguridad:** Conjunto de herramientas, políticas, conceptos, salvaguardas, directrices, métodos de gestión de riesgos, acciones, capacitación y tecnologías que pueden utilizarse para proteger el entorno cibernético, la organización y los activos del usuario.
- **Confidencialidad:** Propiedad de que la información no se pone a disposición o se revela a individuos, entidades o procesos no autorizados.
- **Control:** Medida que modifica el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas de naturaleza administrativa, técnica, de gestión o legal.
- **Datos personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a solicitud de una entidad autorizada.
- **Evento de seguridad:** Ocurrencia identificada que indica una posible brecha o falla en los controles de seguridad de la información.
- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Incidente de seguridad:** Evento único o serie de eventos de seguridad inesperados o no deseados que comprometen las operaciones del negocio y amenazan la seguridad de la información.
- **Integridad:** Propiedad de la información relativa a su exactitud y completitud.

- **MSPI:** Modelo de Seguridad y Privacidad de la Información definido por el Ministerio TIC.
- **Riesgo:** Posibilidad de que una amenaza explote una vulnerabilidad para causar pérdida o daño en un activo de información.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **Seguridad digital:** Área de la informática enfocada en la protección de la infraestructura computacional y la información contenida o circulante.
- **Teletrabajo:** Modalidad de trabajo a distancia que se desarrolla fuera de las instalaciones de la entidad utilizando medios tecnológicos.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

8. ROLES Y RESPONSABILIDADES

La gestión de la seguridad digital en AGUAS DEL CESAR S.A. E.S.P. involucra a todos los niveles de la organización. A continuación, se definen los roles principales:

8.1 Gerencia General

- Aprobar la Política de Seguridad Digital y sus actualizaciones.
- Garantizar la asignación de recursos para la implementación del SGSI.
- Liderar el compromiso institucional con la seguridad de la información.
- Promover la cultura de seguridad digital en la entidad.

8.2 Dirección Administrativa y de Gestión Humana

- Supervisar la implementación de las políticas de seguridad en los procesos administrativos y financieros.
- Facilitar los recursos presupuestales para la gestión de seguridad digital.

8.3 Oficina de Sistemas (Oficial de Seguridad de la Información)

- Coordinar la implementación, mantenimiento y mejora continua del SGSI.
- Administrar los riesgos de seguridad de la información y seguridad digital.
- Gestionar los incidentes de seguridad de la información.
- Realizar el seguimiento al cumplimiento de las políticas de seguridad digital.
- Elaborar y ejecutar los planes de sensibilización y capacitación en seguridad digital.
- Reportar incidentes al CSIRT y al ColCERT según corresponda.

- Mantener actualizado el inventario de activos de información.

8.4 Líderes de Proceso

- Identificar los activos de información de su proceso.
- Ejecutar, diseñar, implementar y monitorear los controles de seguridad asignados.
- Gestionar los riesgos de seguridad digital en el día a día de sus procesos.
- Reportar oportunamente los incidentes de seguridad a la Oficina de Sistemas.

8.5 Oficina de Control Interno

- Proporcionar aseguramiento independiente y objetivo sobre la eficacia del SGSI.
- Realizar auditorías internas al SGSI según el plan de auditoría aprobado.
- Evaluar el cumplimiento de las políticas de seguridad digital.

8.6 Todos los Servidores Públicos, Contratistas y Terceros

- Conocer y cumplir las políticas de seguridad digital de la entidad.
- Participar en las actividades de sensibilización y capacitación en seguridad de la información.
- Reportar de manera inmediata cualquier incidente, evento o debilidad de seguridad detectada.
- Proteger la información de la entidad a la que tengan acceso en razón de sus funciones.
- Hacer uso adecuado de los recursos tecnológicos asignados.

9. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DIGITAL

A continuación, se establecen las políticas específicas de seguridad digital, organizadas por dominio de acuerdo con la norma ISO/IEC 27001:2013 y el MSPI de MinTIC. Cada política define su objetivo y las directrices que deben ser observadas por todos los destinatarios.

9.1 Política de Organización Interna de la Seguridad Digital

Objetivo: Establecer un marco de gestión para iniciar y controlar la implementación de la seguridad digital al interior de la entidad, definiendo roles, responsabilidades, separación de deberes y coordinación con autoridades y partes interesadas.

Directrices:

- La seguridad digital es liderada por la Gerencia General con apoyo de la Dirección Administrativa y Financiera y la Oficina de Sistemas.

- Se designará un responsable de la seguridad de la información (Oficial de Seguridad) con funciones claramente definidas.
- Se implementará la separación de deberes para reducir la posibilidad de uso indebido de los activos de información.
- Se mantendrá contacto con las autoridades competentes en materia de seguridad digital, incluyendo el CSIRT, ColCERT y la Policía Nacional.
- La seguridad de la información se incorporará en la gestión de todos los proyectos de la entidad.
- Las políticas serán revisadas cuando ocurran cambios significativos.

9.2 Política de Sensibilización, Educación y Toma de Conciencia

Objetivo: Promover una cultura de seguridad digital en todos los niveles de la entidad mediante programas de sensibilización, capacitación y comunicación continua.

Directrices:

- Se elaborará y ejecutará un plan anual de sensibilización y capacitación en seguridad de la información dirigido a todos los servidores y contratistas.
- Se realizarán campañas periódicas sobre buenas prácticas de ciberseguridad, prevención de phishing, uso seguro de contraseñas y manejo adecuado de la información.
- Se socializarán las políticas de seguridad digital al momento de la vinculación de personal y contratistas.
- Se realizarán ejercicios simulados de ingeniería social periódicamente para evaluar el nivel de conciencia del personal.
- Los resultados de las actividades de sensibilización serán medidos mediante indicadores de eficacia.

9.3 Política de Gestión de Activos de Información

Objetivo: Identificar, clasificar, valorar y proteger los activos de información de la entidad de acuerdo con su criticidad e importancia.

Directrices:

- Se mantendrá un inventario actualizado de todos los activos de información de la entidad, incluyendo información, software, hardware, servicios, personas e intangibles.

- Cada activo de información tendrá un propietario designado responsable de su protección.
- La información se clasificará conforme a la Ley 1712 de 2014 y la Ley 1581 de 2012 en: pública, clasificada y reservada.
- Se implementarán mecanismos de etiquetado y manejo de la información según su nivel de clasificación.
- Los activos de información se valorarán en términos de confidencialidad, integridad y disponibilidad.
- Al finalizar la vinculación, todos los activos deben ser devueltos y el acceso revocado oportunamente.

9.4 Política de Control de Acceso

Objetivo: Limitar el acceso a la información, a las instalaciones de procesamiento y a los servicios tecnológicos, garantizando que solo las personas autorizadas accedan a los recursos que requieren para el cumplimiento de sus funciones.

Directrices:

- Se establecerá una política de control de acceso basada en el principio de mínimo privilegio y necesidad de conocer.
- La gestión de usuarios incluirá procedimientos formales de registro, modificación y eliminación de cuentas.
- Las contraseñas deben cumplir estándares de complejidad: mínimo 12 caracteres, combinación de mayúsculas, minúsculas, números y caracteres especiales.
- Las contraseñas deben ser cambiadas periódicamente y no podrán ser reutilizadas en las últimas 5 iteraciones.
- Se implementará autenticación multifactor para el acceso a sistemas críticos y acceso remoto.
- Se realizarán revisiones periódicas de los derechos de acceso de los usuarios, como mínimo cada seis meses.
- Queda prohibido compartir credenciales de acceso (usuario y contraseña) entre usuarios.
- Los accesos serán revocados de manera inmediata al término de la vinculación o del contrato.

9.5 Política de Seguridad Física y del Entorno

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la entidad.

Directrices:

- Se definirán áreas seguras con perímetros de seguridad física para proteger la infraestructura crítica de TI (centro de datos, cuartos de comunicaciones).
- El acceso a las áreas seguras estará restringido a personal autorizado mediante controles de acceso físico.
- Se llevará un registro de acceso a las áreas seguras con fecha, hora e identificación de la persona.
- Los equipos de procesamiento de información estarán protegidos contra fallas de suministro eléctrico, inundaciones, incendios y otras amenazas ambientales.
- El cableado de energía y telecomunicaciones estará protegido contra interceptación o daño.
- Se realizará mantenimiento preventivo y correctivo de los equipos de acuerdo con las especificaciones del fabricante.

9.6 Política de Seguridad de las Operaciones

Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información de la entidad.

Directrices:

- Se documentarán los procedimientos operacionales y se pondrán a disposición de los usuarios que los necesiten.
- Los cambios en la organización, los procesos de negocio y los sistemas de información serán controlados mediante un procedimiento formal de gestión de cambios.
- Se implementarán mecanismos de protección contra software malicioso (antivirus, antimalware) en todos los equipos de la entidad.
- Se realizarán copias de respaldo (backups) de la información crítica de acuerdo con un plan de respaldo documentado y probado periódicamente.
- Se registrarán y monitorearán los eventos de seguridad mediante registros de auditoría (logs).
- Se implementará la separación de ambientes de desarrollo, pruebas y producción.
- Se realizarán evaluaciones de vulnerabilidades técnicas y se aplicarán parches y actualizaciones de seguridad de manera oportuna.
- Se restringirá la instalación de software no autorizado en los equipos de la entidad.

9.7 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas

Objetivo: Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo su ciclo de vida.

Directrices:

- Los requisitos de seguridad de la información se incluirán en las especificaciones de nuevos sistemas de información o mejoras a los existentes.
- Se implementarán prácticas de desarrollo seguro de software en todo el ciclo de vida de desarrollo.
- Los cambios en los sistemas de información serán gestionados mediante un procedimiento formal de control de cambios.
- Se realizarán pruebas de seguridad (pruebas de penetración, análisis de código) antes de la puesta en producción de los sistemas.
- Se protegerán los datos de prueba, especialmente cuando contengan datos personales o información sensible.
- Los sistemas adquiridos a terceros deberán cumplir con los estándares de seguridad definidos por la entidad.

9.8 Política de Seguridad en la Relación con Proveedores

Objetivo: Asegurar la protección de los activos de información de la entidad que sean accesibles a los proveedores y terceros.

Directrices:

- Se incluirán cláusulas de seguridad de la información y confidencialidad en todos los contratos con proveedores que accedan a información de la entidad.
- Se evaluará la capacidad de seguridad de los proveedores antes de la contratación.
- Se verificará que los proveedores cumplan con las políticas de ciberseguridad internas de la entidad.
- Se supervisará y revisará periódicamente la prestación de servicios de los proveedores en materia de seguridad.
- Se establecerán acuerdos de nivel de servicio que incluyan requisitos de seguridad de la información.
- Al finalizar la relación contractual, se asegurará la devolución o destrucción segura de la información entregada al proveedor.

9.9 Política de Gestión de Incidentes de Seguridad de la Información

Objetivo: Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.

Directrices:

- Se establecerá y documentará un procedimiento formal de gestión de incidentes de seguridad que incluya las fases de detección, reporte, evaluación, respuesta, recuperación y lecciones aprendidas.
- Todos los servidores y contratistas están obligados a reportar de manera inmediata cualquier incidente o evento de seguridad a la Oficina de Sistemas.
- Se mantendrá un registro de incidentes de seguridad con la información necesaria para su análisis y seguimiento.
- Los incidentes serán clasificados por niveles de severidad y se establecerán tiempos de respuesta acordes.
- Se reportarán los incidentes críticos al CSIRT Gobierno de MinTIC según los protocolos establecidos.
- Se realizarán ejercicios de simulación de incidentes de seguridad digital periódicamente.
- Se recopilarán y preservarán las evidencias digitales cumpliendo la cadena de custodia para posibles investigaciones.

9.10 Política de Continuidad de Negocio y Seguridad de la Información

Objetivo: Asegurar la disponibilidad de la información y la continuidad de los servicios críticos de la entidad en situaciones adversas, crisis o desastres.

Directrices:

- Se elaborará un Plan de Continuidad de Negocio (BCP) que incluya los aspectos de seguridad de la información.
- Se identificarán los servicios y sistemas críticos para la operación de los servicios de agua potable y saneamiento básico.
- Se definirán los tiempos de recuperación objetivo (RTO) y los puntos de recuperación objetivo (RPO) para los sistemas críticos.
- Se implementarán mecanismos de redundancia y respaldo para la infraestructura crítica de TI.

- Se realizarán pruebas y simulacros del plan de continuidad al menos una vez al año.
- Se garantizará la continuidad de la seguridad de la información durante y después de los eventos adversos.

9.11 Política de Seguridad de los Recursos Humanos

Objetivo: Asegurar que los servidores públicos, contratistas y terceros comprendan sus responsabilidades de seguridad de la información durante todo el ciclo de vinculación.

Directrices:

- Se realizarán verificaciones de antecedentes de acuerdo con la normatividad aplicable antes de la vinculación.
- Los contratos de trabajo y los contratos de prestación de servicios incluirán cláusulas de confidencialidad y responsabilidad en seguridad de la información.
- Los servidores y contratistas recibirán inducción en seguridad de la información al inicio de su vinculación.
- Se aplicarán procesos disciplinarios establecidos ante incumplimientos de las políticas de seguridad.
- Al término de la vinculación, se revocarán todos los accesos y se asegurará la devolución de los activos de información.

9.12 Política de Dispositivos Móviles, Teletrabajo y Trabajo Remoto

Objetivo: Establecer los lineamientos para el uso seguro de dispositivos móviles y para la protección de la información en las modalidades de teletrabajo y trabajo remoto.

Directrices:

- Los dispositivos móviles asignados por la entidad deberán contar con software de protección (antivirus, cifrado, bloqueo remoto).
- Queda prohibido almacenar información clasificada o reservada en dispositivos móviles personales sin autorización.
- Los servidores en modalidad de teletrabajo o trabajo remoto deberán utilizar conexiones VPN para acceder a los sistemas de la entidad.
- Se prohíbe el uso de redes Wi-Fi públicas no seguras para acceder a información de la entidad.
- Los equipos utilizados para teletrabajo deberán cumplir con los estándares mínimos de seguridad definidos por la Oficina de Sistemas.
- Se aplicarán las mismas políticas de seguridad de la información independientemente de la ubicación física del colaborador.

9.13 Política de Escritorio Limpio y Pantalla Limpia

Objetivo: Reducir el riesgo de acceso no autorizado, pérdida y daño de la información mediante prácticas de escritorio limpio y pantalla limpia.

Directrices:

- Los documentos impresos con información clasificada o reservada deben ser retirados de los escritorios al finalizar la jornada laboral y almacenados en lugares seguros.
- Las pantallas de los equipos deberán bloquearse automáticamente después de un período de inactividad no mayor a 5 minutos.
- Los usuarios deben bloquear su sesión manualmente al retirarse de su puesto de trabajo, incluso por períodos breves.
- No se deberán dejar notas adhesivas con contraseñas u otra información sensible en los monitores o escritorios.
- Las impresoras compartidas deberán ser revisadas para retirar documentos impresos de manera oportuna.

9.14 Política de Cumplimiento de Requisitos Legales y Contractuales

Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información.

Directrices:

- Se identificarán, documentarán y mantendrán actualizados los requisitos legales y contractuales pertinentes en materia de seguridad de la información.
- Se garantizará el cumplimiento de la Ley 1581 de 2012 de protección de datos personales y sus decretos reglamentarios.
- Se cumplirá con los lineamientos de la Ley 1712 de 2014 de transparencia y acceso a la información pública.
- Se protegerán los derechos de propiedad intelectual y de autor, utilizando únicamente software licenciado y legal.
- Se preservarán los registros de acuerdo con los requisitos legales, regulatorios y contractuales.

9.15 Política de Uso Adecuado de los Recursos Tecnológicos

Objetivo: Garantizar la protección de la información de la entidad a través del buen uso de los recursos tecnológicos asignados a los servidores y contratistas.

Directrices:

- Los recursos tecnológicos (computadores, impresoras, redes, internet, correo electrónico) son propiedad de la entidad y deben ser utilizados exclusivamente para fines institucionales.
- Queda prohibida la instalación de software no autorizado, la descarga de contenido ilegal y el acceso a sitios web de contenido inapropiado.
- El correo electrónico institucional será utilizado únicamente para actividades laborales y no deberá usarse para enviar cadenas, correo masivo no autorizado o información personal sensible.
- El acceso a internet se monitoreará y se aplicarán filtros de contenido para prevenir el acceso a sitios maliciosos o no productivos.
- Los usuarios son responsables de la información que almacenan en los equipos asignados y deben realizar copias de respaldo de su información crítica en los repositorios institucionales.
- Queda prohibido conectar dispositivos personales a la red corporativa sin autorización de la Oficina de Sistemas.

9.16 Política de Clasificación y Etiquetado de la Información

Objetivo: Establecer una metodología para la clasificación, etiquetado y manejo adecuado de la información, conforme a la normatividad colombiana vigente.

Directrices:

- Toda la información de la entidad deberá ser clasificada de acuerdo con la Ley 1712 de 2014 en: información pública, información pública clasificada e información pública reservada.
- Los datos personales se clasificarán conforme a la Ley 1581 de 2012 en: datos públicos, semiprivados, privados y sensibles.
- Cada líder de proceso es responsable de clasificar la información de sus activos.
- Se implementarán mecanismos de etiquetado (físico y digital) conforme a la clasificación otorgada.
- El manejo, almacenamiento, transmisión y disposición final de la información deberá realizarse de acuerdo con su nivel de clasificación.

9.17 Política de Gestión de Riesgos de Seguridad Digital

Objetivo: Establecer el enfoque de gestión de riesgos de seguridad digital de la entidad, alineado con la norma ISO 31000:2018 y la guía del DAFP.

Directrices:

- Se implementará una metodología de gestión de riesgos de seguridad digital que incluya la identificación, análisis, evaluación, tratamiento, monitoreo y revisión de los riesgos.
- Se elaborará y mantendrá actualizado el Plan de Tratamiento de Riesgos de Seguridad de la Información.
- Los riesgos en niveles Alto y Extremo requerirán tratamiento obligatorio; los riesgos en niveles inferiores podrán ser aceptados por la entidad.
- Cada líder de proceso es responsable de identificar y gestionar los riesgos de seguridad digital en sus procesos.
- Se realizará la valoración de riesgos al menos una vez al año o cuando se presenten cambios significativos.
- Se considerarán tanto las amenazas y vulnerabilidades técnicas como las derivadas de factores humanos, organizacionales y del entorno.

9.18 Política de Protección de Datos Personales

Objetivo: Garantizar la protección de los datos personales que la entidad recolecta, almacena, procesa y transmite, en cumplimiento de la Ley 1581 de 2012.

Directrices:

- Se implementarán los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso restringido, seguridad y confidencialidad en el tratamiento de datos personales.
- Se obtendrá la autorización previa, expresa e informada del titular para el tratamiento de sus datos personales.
- Se registrarán las bases de datos personales ante la Superintendencia de Industria y Comercio (SIC) conforme a la normatividad vigente.
- Se garantizarán los derechos de los titulares de datos personales: conocer, actualizar, rectificar y solicitar la supresión de sus datos.
- Se implementarán medidas técnicas, administrativas y humanas para la protección de los datos personales contra accesos no autorizados, pérdida o alteración.
- Se designará un responsable del tratamiento de datos personales en la entidad.

9.19 Política de Seguridad en la Nube

Objetivo: Definir los requisitos de seguridad de la información para los servicios en la nube utilizados por la entidad.

Directrices:

- Antes de adoptar servicios en la nube, se realizará una evaluación de riesgos que considere la ubicación de los datos, jurisdicción aplicable y capacidades de seguridad del proveedor.
- Se incluirán requisitos de seguridad, privacidad y disponibilidad en los contratos con proveedores de servicios en la nube.
- La información clasificada o reservada solo se alojará en servicios en la nube que cuenten con certificaciones de seguridad reconocidas (ISO 27001, SOC 2).
- Se implementarán controles de acceso, cifrado y monitoreo para la información almacenada en la nube.
- Se establecerán procedimientos de respaldo y recuperación para los datos en la nube.
- Se garantizará la portabilidad de los datos al finalizar la relación con el proveedor de nube.

10. SANCIONES POR INCUMPLIMIENTO

El incumplimiento de las políticas de seguridad digital establecidas en el presente documento podrá generar las siguientes consecuencias:

- Para servidores públicos: se aplicarán las acciones disciplinarias previstas en la normatividad vigente, incluyendo el Código General Disciplinario (Ley 1952 de 2019).
- Para contratistas: se aplicarán las sanciones contractuales previstas, pudiendo llegar a la terminación anticipada del contrato.
- Para terceros y proveedores: se aplicarán las cláusulas contractuales acordadas, incluyendo la restricción de acceso y la terminación del acuerdo.

En todos los casos, se informará al jefe inmediato, a la Oficina de Sistemas, a la secretaria General y a la Oficina de Control Interno para la revisión del caso y la adopción de las medidas correspondientes. Lo anterior, sin perjuicio de las acciones penales a que hubiere lugar conforme a la Ley 1273 de 2009 de delitos informáticos.

11. VIGENCIA Y REVISIÓN

La presente Política de Seguridad Digital entrará en vigencia a partir de su aprobación por la Gerencia General de AGUAS DEL CESAR S.A. E.S.P. mediante acto administrativo interno.

Esta política será revisada y actualizada:

- Cuando se presenten cambios significativos en la normatividad aplicable.
- Cuando se identifiquen cambios en el contexto interno o externo de la entidad que afecten la seguridad de la información.
- Cuando los resultados de auditorías o evaluaciones así lo requieran.
- Cuando se materialicen incidentes de seguridad que evidencien la necesidad de ajustes.

Las modificaciones serán aprobadas por la Gerencia General y socializadas a todos los servidores, contratistas y partes interesadas de la entidad.

12. PUBLICACIÓN Y DIVULGACIÓN

La presente política será publicada en la página web institucional de la entidad (www.aguasdelcesar.gov.co) y en los medios internos de comunicación. Se socializará a todos los servidores públicos, contratistas y partes interesadas mediante los canales de comunicación de la entidad.

En caso de modificación o actualización, se realizará una nueva publicación y socialización por los medios dispuestos.

14. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio
1.0	Marzo de 2026	Creación del documento. Versión inicial de la Política de Seguridad Digital de Aguas del Cesar S.A. E.S.P.

15. REGISTRO DE APROBACIÓN

Elaboró	Revisó	Aprobó
Nombre: JONATHAN CASADIEGO AARON Cargo: Profesional en Recursos Informáticos	JANOS CONSULTORES – EDUARD GÓMEZ RAMOS Cargo: Director Administrativo y Financiero	Comité de Gestión y Desempeño